PAT-NO: JP411027311A
DOCUMENT-IDENTIFIER: JP 11027311 A
TITLE: INFORMATION PROCESSING UNIT, ELECTRONIC MAIL METHOD AND MEDIUM
PUBN-DATE: January 29, 1999
INVENTOR-INFORMATION:
NAME
KANEHARA, KATSUMI
INT-CL (IPC): H04L012/54, H04L012/58 , G06F013/00 , H04L009/12 , H04L009/14

ABSTRACT:

PROBLEM TO BE SOLVED: To improve the security by employing the information processing unit provided with plural encryption means where kinds and contents of encryption differ from each other and selecting any of plural the encryption means based on an information content described in a header part of an electronic mail for encryption of a main text of the electronic mail being a transmission object.

SOLUTION: Base addresses for plural kinds of encryption programs are stored in an encryption system entry table in an ROM 2. An MPU 1 extracts a character code stream in a SUBJECT column of header information of an electronic mail generated in an RAM 3, then acquires a base address for the encryption system entry table and generates a storage address of an encryption program by adding lower 2 digits of a sum of the character code stream to the base address. Then the encryption program corresponding to the storage address is acquired from the ROM 2 to encrypt main text information of the electronic mail generated in the RAM 3. Thus, decoding of the encrypted text is made difficult to enhance the security.

(19)日本国特許庁（J.P）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－27311

(43)公開日　平成11年(1999) 1月29日

(51)Int.Cl.[6]		識別記号	FI		
H04L	12/54		H04L	11/20	101B
	12/58		G06F	13/00	351G
G06F	13/00	351	H04L	9/00	631
H04L	9/12				641
	9/14				

審査請求　未請求　請求項の数17　OL　（全 10 頁）

(21)出願番号　特願平9－174951

(22)出願日　平成9年(1997) 6月30日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子3丁目30番2号

(72)発明者　金原　勝美
東京都大田区下丸子3丁目30番2号　キヤノン株式会社内

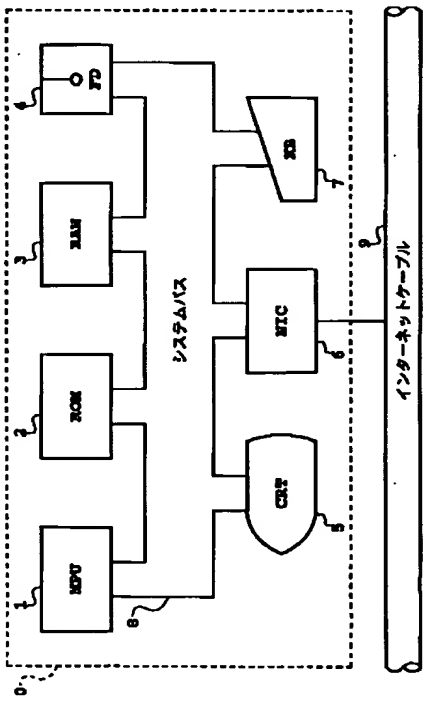
(74)代理人　弁理士　谷　義一　（外1名）

(54)【発明の名称】　情報処理装置および電子メール方法ならびに記録媒体

(57)【要約】

【課題】　電子メールのセキュリティを向上する。

【解決手段】　複数の暗号化プログラムをROM2内に用意しておき、送信対象の電子メールのヘッダ部の記載内容、たとえば、文字コードの総和から、上記複数の暗号化プログラムの1つをMPU1により選択して、電子メールの本文を暗号化する。



1

【特許請求の範囲】

【請求項1】　電子メールの本文を暗号化して他の装置に送信可能な情報処理装置において、

前記電子メールの本文を暗号化することが可能で、暗号化の種類内容がそれぞれ異なる複数の暗号化手段と、

電子メールのヘッダ部に記載された情報内容に基づき前記複数の暗号化手段の1つを送信対象の電子メールの本文の暗号化のために選択する選択手段とを具えたことを特徴とする情報処理装置。

【請求項2】　請求項1に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの総和を前記複数の暗号化手段の1つを選択するための決定要素とすることを特徴とする情報処理装置。

【請求項3】　請求項1に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの文字数を前記複数の暗号化手段の1つを選択するための決定要素とすることを特徴とする情報処理装置。

【請求項4】　請求項1に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載されたメールアドレスの個数を前記複数の暗号化手段の1つを選択するための決定要素とすることを特徴とする情報処理装置。

【請求項5】　請求項1に記載の情報処理装置において、前記複数の暗号化手段は、複数の暗号化プログラムを格納する記憶手段を有し、前記選択手段は、前記ヘッダ部に記載された情報内容から前記記憶手段の記憶アドレスを決定することを特徴とする情報処理装置。

【請求項6】　電子メールの暗号化された本文を他の装置から受信して復号化可能な情報処理装置において、

対応する暗号化方法により暗号化された前記電子メールの本文を復号化することが可能で、復号化の種類内容がそれぞれ異なる複数の復号化手段と、

電子メールのヘッダ部に記載された情報内容に基づき前記複数の復号化手段の1つを送信対象の電子メールの本文の復号化のために選択する選択手段とを具えたことを特徴とする情報処理装置。

【請求項7】　請求項6に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの総和を前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする情報処理装置。

【請求項8】　請求項6に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの文字数を前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする情報処理装置。

【請求項9】　請求項6に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された

2

メールアドレスの個数を前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする情報処理装置。

【請求項10】　請求項6に記載の情報処理装置において、前記複数の復号化手段は、複数の復号化プログラムを格納する記憶手段を有し、前記選択手段は、前記ヘッダ部に記載された情報内容から前記記憶手段の記憶アドレスを決定することを特徴とする情報処理装置。

【請求項11】　第1の情報処理装置で電子メールの本文を暗号化し、第1の情報処理装置から第2の情報処理装置に、本文が暗号化された電子メールを送信し、該第2の情報処理装置で暗号された本文を復号化する電子メール方法において、前記第1の情報処理装置は、前記電子メールの本文を暗号化することが可能で、暗号化の種類内容がそれぞれ異なる複数の暗号化手段を有し、

前記第2の情報処理装置は、前記電子メールの本文を復号化することが可能で、復号化の種類内容がそれぞれ異なる複数の復号化手段を有し、

前記第1の情報処理装置は、電子メールのヘッダ部に記載された情報内容に基づき前記複数の暗号化手段の1つを送信対象の電子メールの本文の暗号化のために選択し、

当該選択された暗号化手段により前記本文を暗号化して送信し、

前記第2の情報処理装置は、受信した電子メールのヘッダ部に記載された情報内容に基づき、前記復号化手段の1つを受信した電子メールの本文の復号化のために選択し、

当該選択した復号化手段により前記電子メールの本文を復号化することを特徴とする電子メール方法。

【請求項12】　請求項11に記載の電子メール方法において、前記ヘッダ部の特定欄に記載された文字コードの総和を前記複数の暗号化手段の1つおよび前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする電子メール方法。

【請求項13】　請求項11に記載の電子メール方法において、前記ヘッダ部の特定欄に記載された文字コードの文字数を前記複数の暗号化手段の1つおよび前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする電子メール方法。

【請求項14】　請求項11に記載の電子メール方法において、前記ヘッダ部の特定欄に記載されたメールアドレスの個数を前記複数の暗号化手段の1つおよび前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする電子メール方法。

【請求項15】　請求項11に記載の電子メール方法において、前記複数の暗号化手段は、複数の暗号化プログラムを格納する記憶手段を有し、前記第1の情報処理装置は、前記ヘッダ部に記載された情報内容から前記記憶手段の記憶アドレスを決定することを特徴とする電子メ

ール方法。

【請求項16】　請求項11に記載の電子メール方法において、前記複数の復号化手段は、複数の復号化プログラムを格納する記憶手段を有し、前記第2の情報処理装置は、前記ヘッダ部に記載された情報内容から該記憶手段の記憶アドレスを決定することを特徴とする電子メール方法。

【請求項17】　請求項1～請求項10のいずれかに記載の情報処理装置の機能をコンピュータにより実行可能なプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置に関するもので、特に文字処理装置とローカルエリアネットワーク（LAN）のネットワークサーバとの間で、電子メールの送受信を行い、電子メールにセキュリティを付加する情報処理装置および電子メール方法ならびに記録媒体に関する。

【0002】

【従来の技術】近年、文字処理技術、通信技術、情報処理技術の進歩により、ワードプロセッサやパーソナルコンピュータ等各種の情報処理装置においても、ローカルエリアネットワーク（LAN）を介して電子メールの送受信を行うことが可能になってきた。

【0003】さらにメールの盗聴を防止するために、本文領域に暗号化を施してからメールを送信し、受信側で復号化して読むことが行われているが、暗号、復号方式はそれぞれ1対の方式に限定しているのが一般的な方式であった。

【0004】

【発明が解決しようとする課題】従来例では、暗号化方式が1通りのため、盗聴する側で解読する際、1つ解読キーを見つけると、以後すべてのメールが盗聴されてしまい、また解読の際にも複数のサンプルが簡単に取得できてしまい、解読のキーワードが見つけ易くなるなどの問題点があった。そこで、本発明の目的は、セキュリティ性をより向上させる情報処理装置および電子メール方法ならびに記録媒体を提供することにある。

【0005】

【課題を解決するための手段】このような目的を達成するために、請求項1の発明は、電子メールの本文を暗号化して他の装置に送信可能な情報処理装置において、前記電子メールの本文を暗号化することが可能で、暗号化の種類内容がそれぞれ異なる複数の暗号化手段と、電子メールのヘッダ部に記載された情報内容に基づき前記複数の暗号化手段の1つを送信対象の電子メールの本文の暗号化のために選択する選択手段とを具えたことを特徴とする。

【0006】請求項2の発明は、請求項1に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定

欄に記載された文字コードの総和を前記複数の暗号化手段の1つを選択するための決定要素とすることを特徴とする。

【0007】請求項3の発明は、請求項1に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの文字数を前記複数の暗号化手段の1つを選択するための決定要素とすることを特徴とする。

【0008】請求項4の発明は、請求項1に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載されたメールアドレスの個数を前記複数の暗号化手段の1つを選択するための決定要素とすることを特徴とする。

【0009】請求項5の発明は、請求項1に記載の情報処理装置において、前記複数の暗号化手段は、複数の暗号化プログラムを格納する記憶手段を有し、前記選択手段は、前記ヘッダ部に記載された情報内容から前記記憶手段の記憶アドレスを決定することを特徴とする。

【0010】請求項6の発明は、電子メールの暗号化された本文を他の装置から受信して復号化可能な情報処理装置において、対応する暗号化方法により暗号化された前記電子メールの本文を復号化することが可能で、復号化の種類内容がそれぞれ異なる複数の復号化手段と、電子メールのヘッダ部に記載された情報内容に基づき前記複数の復号化手段の1つを送信対象の電子メールの本文の復号化のために選択する選択手段とを具えたことを特徴とする。

【0011】請求項7の発明は、請求項6に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの総和を前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする。

【0012】請求項8の発明は、請求項6に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載された文字コードの文字数を前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする。

【0013】請求項9の発明は、請求項6に記載の情報処理装置において、前記選択手段は前記ヘッダ部の特定欄に記載されたメールアドレスの個数を前記複数の復号化手段の1つを選択するための決定要素とすることを特徴とする。

【0014】請求項10の発明は、請求項6に記載の情報処理装置において、前記複数の復号化手段は、複数の復号化プログラムを格納する記憶手段を有し、前記選択手段は、前記ヘッダ部に記載された情報内容から前記記憶手段の記憶アドレスを決定することを特徴とする。

【0015】請求項11の発明は、第1の情報処理装置で電子メールの本文を暗号化し、第1の情報処理装置から第2の情報処理装置に、本文が暗号化された電子メー

5

ルを送信し、該第２の情報処理装置で暗号された本文を復号化する電子メール方法において、前記第１の情報処理装置は、前記電子メールの本文を暗号化することが可能で、暗号化の種類内容がそれぞれ異なる複数の暗号化手段を有し、前記第２の情報処理装置は、前記電子メールの本文を復号化することが可能で、復号化の種類内容がそれぞれ異なる複数の復号化手段を有し、前記第１の情報処理装置は、電子メールのヘッダ部に記載された情報内容に基づき前記複数の暗号化手段の１つを送信対象の電子メールの本文の暗号化のために選択し、当該選択された暗号化手段により前記本文を暗号化して送信し、前記第２の情報処理装置は、受信した電子メールのヘッダ部に記載された情報内容に基づき、前記復号化手段の１つを受信した電子メールの本文の復号化のために選択し、当該選択した復号化手段により前記電子メールの本文を復号化することを特徴とする。

【００１６】請求項１２の発明は、請求項１１に記載の電子メール方法において、前記ヘッダ部の特定欄に記載された文字コードの総和を前記複数の暗号化手段の１つおよび前記複数の復号化手段の１つを選択するための決定要素とすることを特徴とする。

【００１７】請求項１３の発明は、請求項１１に記載の電子メール方法において、前記ヘッダ部の特定欄に記載された文字コードの文字数を前記複数の暗号化手段の１つおよび前記複数の復号化手段の１つを選択するための決定要素とすることを特徴とする。

【００１８】請求項１４の発明は、請求項１１に記載の電子メール方法において、前記ヘッダ部の特定欄に記載されたメールアドレスの個数を前記複数の暗号化手段の１つおよび前記複数の復号化手段の１つを選択するための決定要素とすることを特徴とする。

【００１９】請求項１５の発明は、請求項１１に記載の電子メール方法において、前記複数の暗号化手段は、複数の暗号化プログラムを格納する記憶手段を有し、前記第１の情報処理装置は、前記ヘッダ部に記載された情報内容から前記記憶手段の記憶アドレスを決定することを特徴とする。

【００２０】請求項１６の発明は、請求項１１に記載の電子メール方法において、前記複数の復号化手段は、複数の復号化プログラムを格納する記憶手段を有し、前記第２の情報処理装置は、前記ヘッダ部に記載された情報内容から該記憶手段の記憶アドレスを決定することを特徴とする。

【００２１】請求項１７の発明は、請求項１～請求項１０のいずれかに記載の情報処理装置の機能をコンピュータにより実行可能なプログラムを記録したことを特徴とする。

【００２２】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態を詳細に説明する。

6

【００２３】図１は本発明に係る文字処理装置のシステム構成を示す。図１において、０は文字処理装置である。

【００２４】文字処理装置０は、以下に説明する構成部を有する。すなわち、文字処理装置０は、本装置全体の制御を実行したり、後述する電子メールの暗号化、復号化を実行するＭＰＵ１、本装置のシステムプログラム、後述するフローチャートの記憶エリアであるＲＯＭ２（リードオンリメモリ）、後述する電子メールのヘッダ領域、本文領域を一時記憶したり、演算、比較の演算データを記憶するためのワークエリアであるＲＡＭ（ランダムアクセスメモリ）３、文字処理装置０で作成した文書、電子メールなどを保存するためのＦＤ（フロッピーディスク）４、オペレータが文書の入力、電子メールのヘッダ情報、本文領域の情報の入力を行ったり、操作の指示を行うＫＢ（キーボード）７、ユーザが入力した文書、電子メールなどを表示するＣＲＴ（ディスプレイ装置）５、文字処理装置０をローカルエリアネットワークと接続するＮＩＣ（ネットワークインタフェースカード）６から構成され、それぞれシステムバス８で接続されている。

【００２５】ローカルエリアネットワーク用の通信ケーブル９はイーサネットと呼ばれる通信ケーブルを使用する。イーサネットケーブル９には、文字処理装置０のメールをスプールするメールサーバ、文字処理装置の通信相手であるネットワーク端末などが数台接続されている。

【００２６】図２はＲＡＭ３へ展開された文字処理装置０のシステムプログラムの構成を示す。図２において、１１はネットワークシステム用のプログラム（以下、ネットワークシステムプログラムと称す）で、本文字処理装置のネットワーク通信に関わる処理全体の状態監視、電子メールの送受信管理、後述する電子メールの暗号化、復号化の処理の管理などを行う。

【００２７】１２は電子メール送信プログラムで、送信するメールの作成、送信先のアドレスの指定、暗号化の有無の管理など、メールを送信する際の一連の処理、および状態管理を行う。１３はヘッダ情報作成プログラムで、メールを送信する際に必要とするヘッダ部分の作成の一連の処理、および状態監視を行う。本実施例においてはヘッダ情報作成プログラムで作成したヘッダ情報（後述するｄａｔａ，ｓｕｂｊｅｃｔ，ｃｃなど）を基に、後述する暗号化方式を決定する。

【００２８】１４は本文領域作成プログラムで、送信するメールの本文領域の文の作成、データの管理などを行う。１５はメール送信プログラムで、電子メールを送信する場合の基本処理、状態監視などを行う。１６は暗号メール送信プログラムで、メール送信プログラム１５で暗号化の指示が発生した場合、メールの暗号化の一連の処理、状態管理などを行う。

【００２９】１７は暗号化方式決定プログラムで、ヘッダ情報作成プログラム１３で作成したヘッダ情報を基に、暗号化の方式を決定する。１８は本文領域暗号化プログラムで、本文領域作成プログラム１４で作成した本文領域の文を、暗号化方式決定プログラム１６で決定した暗号化方式にしたがって、暗号化する。

【００３０】１９は電子メール受信プログラムで、受信メール一覧の作成、メールの受信、メールの復号化の管理など、メールを受信する際の一連の操作、および状態管理を行う。２０は受信メール復号化プログラムで、受信したメールが暗号化されていた場合に、復号化処理の一連の処理、状態管理などを行う。２２は復号化方式決定プログラムで、電子メール受信プログラム１９で受信した電子メールのヘッダ情報を基にして、復号化方式を決定する。２１は本文領域復号化プログラムで、電子メール受信プログラム１９で受信した電子メールの本文領域の文を、復号化方式決定プログラム２２で決定した復号化方式に基づき、復号化する。

【００３１】以上の構成による、本実施形態の処理の機能概略ブロック図を図３に示す。図３はＲＡＭ３に展開されたシステムプログラムの制御手順に従った処理を行うＭＰＵ１の処理機能を示す。

【００３２】以下に述べた機能は図２で説明したプログラムをＭＰＵ１が実行することにより実現される。図３において、まず電子メールの送信側、電子メール送信手段３０は、電子メールの送信を行う場合の周知の基本操作、状態監視等を行う。

【００３３】電子メールヘッダ情報作成手段３１は、電子メール送信手段３０でヘッダ情報作成の操作の指示が発生した場合にこの手段に制御が移り、送信する電子メールのヘッダ情報としてＴＯ：（この後に送信先のメールアドレスがユーザにより記入される。），ＣＣ：（この後に同報通信先のメールアドレスがユーザにより記入される。），ＳＵＢＪＥＣＴ：（この後に文の主題内容がユーザにより記入される。），ＤＡＴＥ：（日付情報）をＲＡＭ３上に形成する。

【００３４】電子メール本文領域作成手段３２は、電子メール送信手段３０で本文領域作成の操作指示が発生した場合にこの手段に制御が移り、電子メールの本文領域ＲＡＭ３上に作成する。メール送信手段３３は、電子メール送信手段３０で電子メールを送信する操作指示が発生した場合にこの手段に制御が移り、暗号化の有無をオペレータに問いかけ、暗号化有の場合、暗号メール送信手段３４に制御を渡す。

【００３５】暗号メール送信手段３４は、メール送信手段３３で暗号化有の操作指示を受けた場合にこの手段に制御が移り、ヘッダ情報作成手段３１で作成したヘッダ情報をパラメータに暗号化方式決定手段３６に制御を渡し、その後、本文領域作成手段３２で作成した本文情報により、本文領域暗号化手段３５に制御を渡す。

【００３６】暗号化方式決定手段３６は、暗号メール送信手段３４から制御を受け、３１のヘッダ情報作成手段でＲＡＭ３上に展開したヘッダ情報を基に、暗号化方式を決定する。本文領域暗号化手段３５は、暗号メール送信手段３４から制御を受け、本文領域手段３２でＲＡＭ３上に展開した本文情報を、暗号化方式決定手段３６で決定した暗号化方式に基づいて、暗号化する。

【００３７】電子メール受信手段３７は、電子メールの受信を行う場合の基本操作、状態監視等を行う。受信メール復号化手段３８は、電子メール受信手段３７で受信した電子メールが暗号化されている場合に制御が移り、電子メール受信手段３７で受信した電子メールのヘッダ情報をパラメータに、復号化方式決定手段３９に制御を渡し、電子メール受信手段３７で受信した電子メールの本文情報により、本文領域復号化手段４０に制御を渡す。

【００３８】復号化方式決定手段３９は、受信メール復号化手段３８から制御を受け、電子メール受信手段３７でＲＡＭ３上に展開したヘッダ情報を基に、復号化方式を決定する。本文領域復号化手段４０は、受信メール復号化手段３８から制御を受け、電子メール受信手段３７でＲＡＭ３上に展開した本文情報を、復号化方式決定手段３９で決定した復号化方式に基づいて、復号化する。

【００３９】以上のシステム構成で実行される電子メールの送受信処理を図４～図１２を参照して説明する。電子メール送信処理のフローを図４に示す。

【００４０】装置に電源が投入されてネットワークシステムプログラム１１へ制御が渡り、電子メール送信処理プログラムへ制御が渡るまでの手順は、従来と同様である。電子メール送信処理では、ＭＰＵ１はまずキーボード７の入力キーの操作内容のチェックを行う（Ｓ５１）。ヘッダ情報作成に関わる情報入力の場合は、ヘッダ情報作成プログラム１３をコールし、ヘッダ情報作成処理を実行し（Ｓ５６）、再び入力キーチェック（Ｓ５１）の処理へ戻る。以下、ユーザが情報入力を行う毎にステップＳ５１→Ｓ５６のループによりヘッダ情報が作成される。

【００４１】ヘッダ情報作成以外の情報入力があった場合は（Ｓ５１のＮＯ判定）、入力キーが本文領域作成に関わる情報を入力したかチェックする（Ｓ５２）。本文領域作成情報入力の場合は、本文領域作成プログラム１４をコールして本文領域作成処理を実行し（Ｓ５７）、再びキー入力の判定処理へ戻る。

【００４２】Ｓ５２でＮＯ判定が得られた場合は、入力キーがメール送信に関わる情報を入力したかをチェックする（Ｓ５３）。メール送信の情報の入力の場合は、メール送信プログラム１５をコールしてメール送信処理を実行し（Ｓ５８）、再びキー入力判定処理へ戻る。

【００４３】Ｓ５３でＮＯ判定が得られた場合は、入力キーが環境設定に関わる情報を入力したかをチェックす

る（Ｓ54）。環境設定の情報への場合は、環境設定処理（プログラム）をコールして環境設定処理を実行し（Ｓ59）、再びキー入力の判定処理へ戻る。Ｓ54でＮＯ判定が得られた場合は、入力キーが終了を指示しているかをチェックする（Ｓ55）。終了の指示の場合はネットワークシステムプログラムへリターン11へする。それ以外の場合は、再びキー入力の判定処理（51）へ戻る。

【0044】次に図4のＳ58のメール送信処理（電子メール送信プログラム12）の詳細を図5に示す。メール送信処理では、ユーザからの暗号化の要求が有るか無いかをチェックする（Ｓ61）。ユーザのキー入力による暗号化の要求がない場合は、従来のメール送信処理をコールし、実行して（Ｓ63）、リターンする。

【0045】暗号化の要求がある場合は、暗号メール送信処理（暗号メール送信プログラム16）をコールして実行し（Ｓ62）、リターンする。

【0046】次に図5のＳ62の暗号メール送信処（暗号メール送信プログラム16）の詳細を図6に示す。暗号メール送信処理では、暗号化方式決定処理をコールしてまずヘッダ情報作成処理（Ｓ56）でＲＡＭ3上に作成した電子メールのヘッダ情報を暗号化方式決定処理に引き渡す（Ｓ71）。この暗号化方式決定処理で複数種の暗号化方式の中で、一つの暗号化方式が選択される。次に暗号化方式決定処理（Ｓ71）で決定した暗号化方式、および本文領域作成処理（Ｓ57）でＲＡＭ3上に作成した電子メールの本文領域をパラメータに本文領域暗号化処理をコールする（Ｓ72）。最後に従来と同様のメール送信処理をコールし（Ｓ73）、暗号化した電子メール（暗号化した本文+ヘッダ）を相手先へ送信する。

【0047】次に図6のＳ71の暗号化方式決定処理の詳細を図7に示す。本実施形態では複数種の暗号化プログラムの記憶アドレスの一部がＲＯＭ2内の暗号化方式エントリーテーブルに記憶されている。

【0048】そこで、暗号化方式決定処理では、ＭＰＵ1はまずヘッダ情報作成処理（Ｓ56）でＲＡＭ3上に作成した電子メールのヘッダ情報のＳＵＢＪＥＣＴ欄に記載された文字コード列を取り出し、各文字コードの操作を求める（Ｓ81）。

【0049】次に後述する暗号化方式エントリーテーブルのベースアドレスを取得する（Ｓ82）。

【0050】そして暗号化方式エントリーテーブルから読み取ったアドレス（ベースアドレス）にＳ81で求めたＳＵＢＪＥＣＴ欄の文字コードの総和の下2桁を加えて暗号化プログラムの記憶アドレス（暗号化方式該当アドレス）を作成する（Ｓ83）。

【0051】そして暗号化方式該当アドレスに対応する暗号化プログラムをＲＯＭ2から取得して（Ｓ84）リターンする。

【0052】次に図6のステップＳ72の本文領域暗号化処理の詳細を図8に示す。本文領域暗号化処理では、まず暗号化方式決定処理（図6のステップＳ71）で決定した暗号化プログラムをロードする（Ｓ91）。

【0053】そして上記暗号化プログラムにより、本文領域作成処理（Ｓ57）でＲＡＭ3上に作成した電子メールの本文情報を暗号化する（Ｓ92）。

【0054】次に電子メール受信処理のフローを図9に示す。装置に電源が投入されると、従来と同様ネットワークシステムプログラム11へ制御が渡り、次に電子メール受信処理（電子メール受信プログラム19）へ制御が引き渡される。図9の電子メール受信処理では、まず従来と同様の電子メール受信処理を行う（Ｓ103）。

【0055】そして受信したメールが暗号化されているか否かチェックし（Ｓ101）、暗号化されている場合は受信メール復号化処理をコールして実行する（Ｓ102）。暗号化の有無の判定方法は、オペレータによる確認、ヘッダに記載された識別情報によるＭＰＵ1の自動判定等を使用することができる。

【0056】次に図9のステップＳ102の電子メール復号化処理の詳細を図10に示す。

【0057】電子メール復号化処理では、電子メール受信処理（Ｓ103）で受信したメールのヘッダ情報をパラメータに設定して復号化方式決定処理（復号化方式決定プログラム22）をコールして、復号化方式を決定する（Ｓ111）。

【0058】次に復号化方式決定処理（Ｓ111）で決定した復号化方式、および電子メール受信処理（Ｓ103）でＲＡＭ3上に受信した電子メールの本文領域をパラメータに、本文領域復号化処理をコールする（Ｓ102）。これにより暗号化された本文領域を暗号化前の文に復号化することが可能となる。

【0059】次に図10のＳ111の復号化方式決定処理の詳細を図11に示す。復号化方式決定処理では、ＭＰＵ1はまず電子メール受信処理（Ｓ103）でＲＡＭ3上に受信した電子メールのヘッダ情報のｓｕｂｊｅｃｔ欄に記載された各文字コードの総和を求める（Ｓ121）。

【0060】次に後述する復号化方式エントリーテーブルのベースアドレスを取得する（Ｓ122）。

【0061】そして復号化方式エントリーテーブルベースアドレスにＳ121で求めたＳＵＢＪＥＣＴ欄の文字コードの総和の下2桁を加える復号化方式該当アドレスを作成する（Ｓ123）。ＭＰＵ1は復号化方式該当アドレスに記憶する復号化プログラムをＲＯＭ2から取得して（Ｓ124）リターンする。

【0062】次に図10のＳ112の本文領域復号化処理の詳細を図12に示す。本文領域復号化処理では、まず復号化方式決定処理（Ｓ111）で決定した復号化プログラムをロードする（Ｓ131）。上記復号化プログ

ラムにより、電子メール受信処理（S103）でRAM3上に受信した電子メールの本文情報を復号化する（S132）。

【0063】次に上述した暗号化方式エントリーテーブル、および暗号化方式該当テーブルの構成を図13に、復号化方式エントリーテーブル、および復号化方式該当テーブルの構成を図14にそれぞれ示す。

【0064】図13の暗号化方式エントリーテーブル、復号化方式エントリーテーブルはそれぞれ1～100までのエントリーポインタを持つ。

【0065】同様に暗号化方式該当テーブル、復号化方式該当テーブルはそれぞれ1～100までの処理方式を定義した暗号化、復号化プログラムが記憶されている。

【0066】そしてメールの送信側と受信側で、各テーブルの処理方式の構成を同じにすることにより、送信側で暗号化したメールを送信すると、受信側で送信側の暗号化方式に対応する復号化方式によりメールを復号化することが可能となる。

【0067】（他の実施例）

1）本実施例では、暗号、復号処理を暗号化方式エントリーテーブル、復号化方式エントリーテーブルにそれぞれ100種類エントリーしたが、処理方式が2種類以上あればよく、エントリーテーブルにランダムに使用可能な処理方式のポインタを設定し、暗号、復号化各エントリーテーブルの対応を取ることにより運用可能となる。

【0068】また、エントリー数を10種類、1000種類と変更すると、暗号化方式決定処理S83、復号化方式決定処理S123のエントリーテーブルに加える変数の桁数を変更することにより運用可能となる。

【0069】その他に図7の暗号化方式決定処理、図8の復号化方式決定処理で各エントリーテーブルの相対位置を電子メールのヘッダ情報のSUBJECT欄の文字コードの総和から求めたが、同じくSUBJECT欄の文字数、CC欄に記載されたメールアドレスの個数、文字コードの総和、文字数、TO欄に記載されたメールアドレスの個数、文字コードの総和、文字数、ヘッダ情報の文字数、文字コードの総和、DATE欄に記載された日付け情報（決定要素）等とエントリーテーブルの相対位置との間の相関関係を定めておき、この相関関係から暗号化プログラムを決定することにより、よりセキュリティに富んだメールシステムを実現することができる。

【0070】2）本実施の形態では、図4～図12のプログラムおよび図13と図14のテーブルをROM2に格納しているが、ハードディスク記憶装置に記憶してもよいし、フロッピディスクやCD－ROMからハードディスク記憶装置にインストールしてもよい。

【0071】

【発明の効果】請求項1、6、11、17の発明では、複数の暗号化手段、復号化手段の中の使用すべき手段が、電子メールのヘッダー部の記載内容から決定される。ヘッダー部の記載内容は、電子メール毎に異なるので、各電子メールで使用される暗号化手段、復号化手段も異なるので、暗号文の解読がより困難となり、よりセキュリティ性が高まる。

【0072】請求項2～4、7～9、12～14の発明では、ヘッダー部の特定欄、たとえば、送り先を記入する欄（TO）や主題を記入する欄（SUBJECT）に記載された文字コードの総和、文字数、あるいは、送り先（TO）や同報通信先欄（CC）に記載するメールアドレスの個数等の示す数値と複数の暗号化手段、復号化手段とを関連付け、この関連付けから暗号化手段、復号化手段を関連付ける。

【0073】このため、暗号化手段や復号化手段自体がたとえ、盗まれても、暗号化された本文がどの暗号化手段を使用したか分からないので、よりセキュリティ性が高まる。

【0074】請求項5、10、15～16の発明では、使用する暗号化プログラム、復号化プログラムを読み出す記憶アドレスがあたかも暗号化され、電子メール用のプログラム中には、暗号化プログラムや復号化プログラムの記憶アドレスが数値の形態で記載されない。このため、リバースエンジニアリング等でプログラム解析を行っても、暗号化プログラムや復号化プログラムの記憶先が不明であり、暗号化プログラムや復号化プログラムが保護される。

【図面の簡単な説明】

【図1】本発明実施の形態のシステム構成を示すブロック図である。

【図2】本発明実施の形態のプログラムの関連を示すブロック図である。

【図3】本発明実施の形態の機能構成を示すブロック図である。

【図4】電子メール送信処理の処理内容を示すフローチャートである。

【図5】メール送信処理の処理内容を示すフローチャートである。

【図6】暗号メール処理の処理内容を示すフローチャートである。

【図7】暗号化方式決定処理の処理内容を示すフローチャートである。

【図8】本文領域暗号化処理の処理内容を示すフローチャートである。

【図9】電子メール受信処理の処理内容を示すフローチャートである。

【図10】受信メール復号化処理の処理内容を示すフローチャートである。

【図11】復号化方式決定処理の処理内容を示すフローチャートである。

【図12】本文領域復号化処理の処理内容を示すフローチャートである。

13　　14

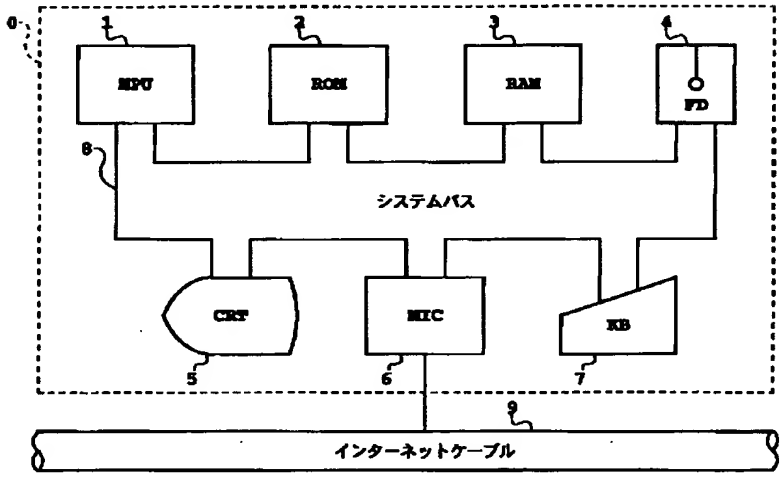
【図13】暗号化エントリーテーブルおよび暗号化方式該当テーブルの構成を示す構成図である。

【図14】復号化エントリーテーブルおよび復号化方式該当テーブルの構成を示す構成図である。

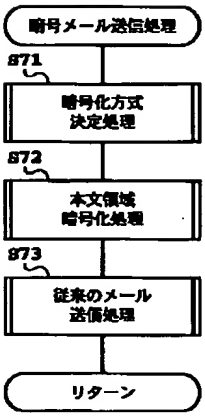
【符号の説明】

1　MPU
2　ROM
3　RAM
4　FD
5　CRT
6　NIC
7　KB

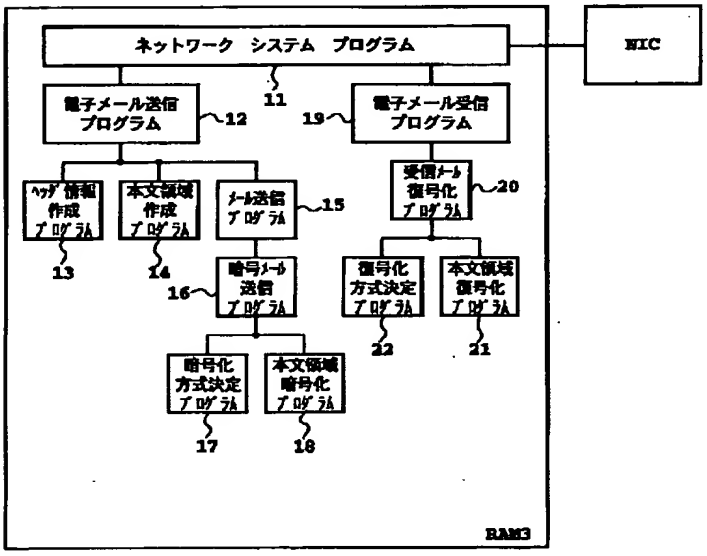
【図1】



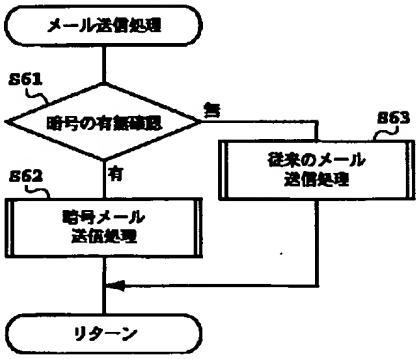
【図6】



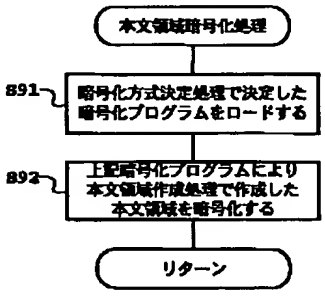
【図2】



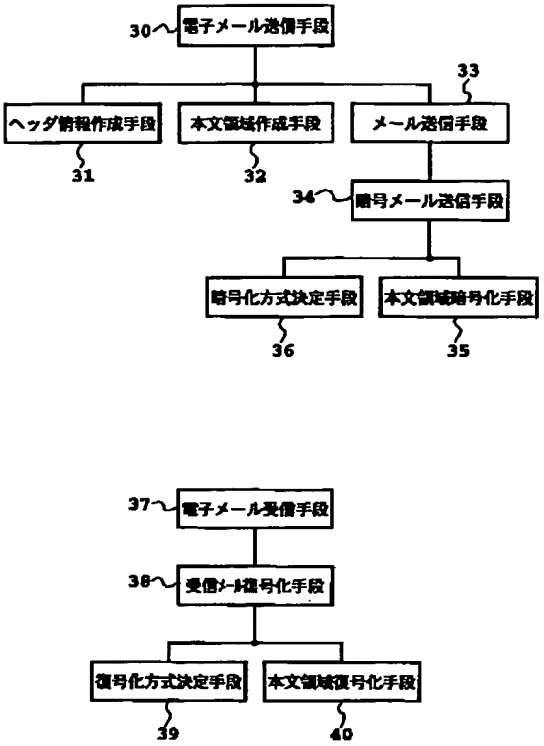
【図5】



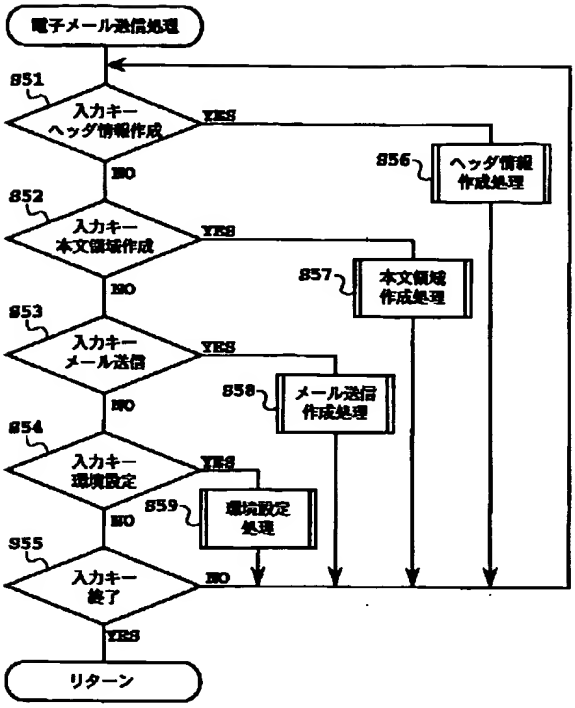
【図8】



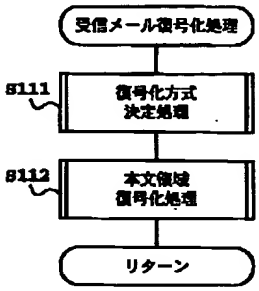
【図3】



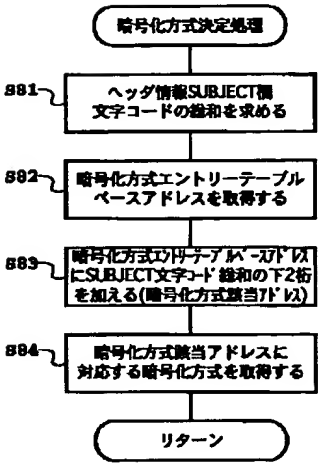
【図4】



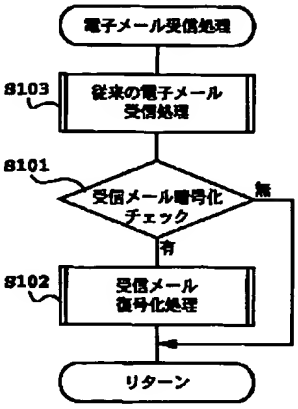
【図10】



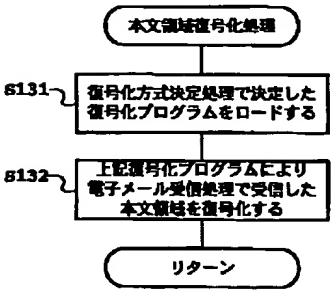
【図7】



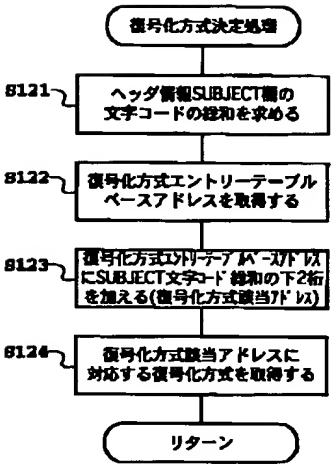
【図9】



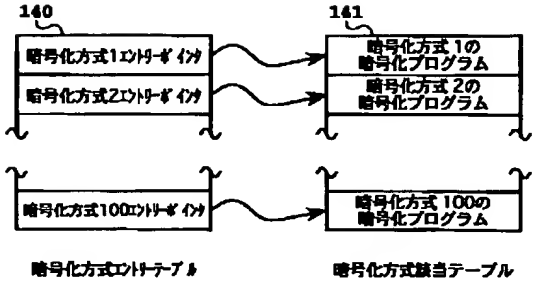
【図12】



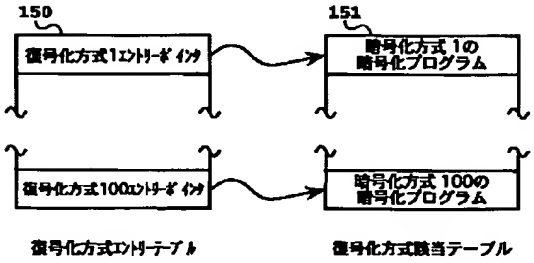
【図11】


復号化方式決定処理
S121
ヘッダ情報SUBJECT欄の
文字コードの総和を求める
S122
復号化方式エントリーテーブル
ベースアドレスを取得する
S123
復号化方式エントリーテーブルベースアドレス
にSUBJECT文字コード総和の下2桁
を加える(復号化方式該当アドレス)
S124
復号化方式該当アドレスに
対応する復号化方式を取得する
リターン

【図13】


140
141
暗号化方式1エントリーポインタ
暗号化方式2エントリーポインタ
暗号化方式100エントリーポインタ
暗号化方式 1の
暗号化プログラム
暗号化方式 2の
暗号化プログラム
暗号化方式 100の
暗号化プログラム
暗号化方式エントリーテーブル
暗号化方式該当テーブル

【図14】


150
151
復号化方式1エントリーポインタ
復号化方式100エントリーポインタ
暗号化方式 1の
暗号化プログラム
暗号化方式 100の
暗号化プログラム
復号化方式エントリーテーブル
復号化方式該当テーブル